

(11)Publication number : 10-268764  
(43)Date of publication of application : 09.10.1998

(21)Application number : 09-077297 (71)Applicant : HITACHI LTD  
(22)Date of filing : 28.03.1997 (72)Inventor : MATSUNAGA KAZUO

[illegible]

Copyright (C): 1998,2003 Japan Patent Office

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-268764

(43) 公開日 平成10年(1998)10月9日

(51) Int.Cl.<sup>6</sup>  
G 0 9 C 1/00  
H 0 4 L 9/32

識別記号  
6 4 0

F I  
G 0 9 C 1/00  
H 0 4 L 9/00

6 4 0 B  
6 7 5 D

審査請求 未請求 請求項の数7 O L (全 9 頁)

(21) 出願番号 特願平9-77297  
(22) 出願日 平成9年(1997)3月28日

(71) 出願人 000005108  
株式会社日立製作所  
東京都千代田区神田駿河台四丁目6番地  
(72) 発明者 松永 和男  
神奈川県横浜市戸塚区戸塚町5030番地 株  
式会社日立製作所ソフトウェア開発本部  
(74) 代理人 弁理士 有近 紳志郎

(54) 【発明の名称】 電子化情報保証方法、保証サーバおよび保証サーバプログラムを記録した記録媒体

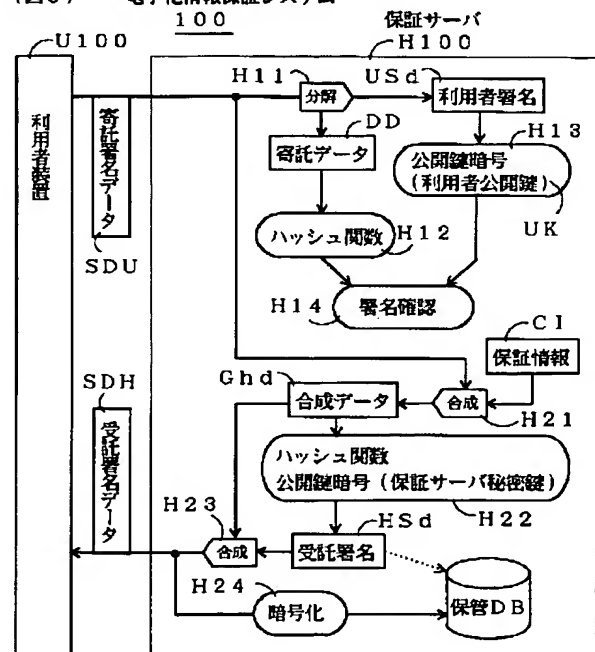
(57) 【要約】

【課題】 過去に作成した電子化情報の内容が変更されていないことを保証する電子化情報保証方法を提供する。

【解決手段】 利用者が電子署名した電子化情報を保証サーバに寄託する。保証サーバは、利用者が電子署名した電子化情報にタイムスタンプなどの保証情報を付加し、電子署名し、さらに暗号化してデータベースに保管する。暗号方法は適宜変更する。後日、利用者は、電子化情報の交付を保証サーバに依頼する。保証サーバは、データベースから電子化情報を読み出し、復号し、交付する。

【効果】 利用者自身の電子署名と保証サーバの電子署名の2重の署名により、内容が変更されていないことを保証できる。

(図6) 電子化情報保証システム



BEST AVAILABLE COPY

**【特許請求の範囲】**

【請求項 1】 利用者が電子化情報を公正な立場と認められる第三者機関に寄託し、第三者機関が前記電子化情報を保管すると共に内容が変更されていないことを保証して当該保管されている電子化情報を利用者に提供することを特徴とする電子化情報保証方法。

【請求項 2】 利用者が電子化情報を公正な立場と認められる第三者機関に寄託し、第三者機関が前記電子化情報のダイジェストを保管すると共に利用者から保証依頼された電子化情報のダイジェストを生成し前記保管していたダイジェストと照合し一致したときに内容が変更されていないことを利用者に保証することを特徴とする電子化情報保証方法。

【請求項 3】 利用者から寄託された電子化情報を保管する保管手段と、保管していた電子化情報とその内容が変更されていないことの電子化保証とを含む電子化保証書を発行する電子化保証書発行手段とを具備することを特徴とする保証サーバ。

【請求項 4】 利用者から寄託された電子化情報のダイジェストを生成し保管する保管手段と、利用者から保証依頼された電子化情報のダイジェストを生成し前記保管していたダイジェストと照合し一致したときに内容が変更されていないことを保証する電子化保証書を発行する電子化保証書発行手段とを具備することを特徴とする保証サーバ。

【請求項 5】 請求項 3 または請求項 4 に記載の保証サーバにおいて、前記保管手段は、電子化情報またはダイジェストを暗号化して保管すると共に、異なる暗号方式により暗号化し直して保管し直すことが可能であることを特徴とする保証サーバ。

【請求項 6】 利用者から寄託された電子化情報を保管する保管手段と、保管していた電子化情報とその内容が変更されていないことの電子化保証とを含む電子化保証書を発行する電子化保証書発行手段とをコンピュータに実現させる保証サーバプログラムを記録した、コンピュータ読み取り可能な記録媒体。

【請求項 7】 利用者から寄託された電子化情報のダイジェストを生成し保管する保管手段と、利用者から保証依頼された電子化情報のダイジェストを生成し前記保管していたダイジェストと照合し一致したときに内容が変更されていないことを保証する電子化保証書を発行する電子化保証書発行手段とをコンピュータに実現させる保証サーバプログラムを記録した、コンピュータ読み取り可能な記録媒体。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】本発明は、電子化情報保証方法、保証サーバおよび保証サーバプログラムを記録した記録媒体に関し、さらに詳しくは、過去に作成した電子化情報の内容が変更されていないことを保証する電子化

情報保証方法、寄託された電子化情報の内容が変更されていないことを利用者に保証する保証サーバおよびその保証サーバの機能をコンピュータに実現させるための保証サーバプログラムを記録した記録媒体に関する。

**【0002】**

【従来の技術】従来、証明機関（Certification Authorities）から発行された証明書を実体的に配布することにより身分を証明する身分証明技術や、作成した電子化情報に電子署名（デジタル署名）を付加することにより当該電子化情報の正当性を証明するメッセージ認証技術が知られている。しかし、過去に作成した電子化情報の内容が変更されていないことを保証する電子化情報保証技術は知られていない。

**【0003】**

【発明が解決しようとする課題】そこで、本発明の第 1 の目的は、過去に作成した電子化情報の内容が変更されていないことを保証する電子化情報保証方法を提供することにある。また、本発明の第 2 の目的は、寄託された電子化情報の内容が変更されていないことを利用者に保証する保証サーバを提供することにある。更に、本発明の第 3 の目的は、上記保証サーバの機能をコンピュータに実現させるための保証サーバプログラムを記録した記録媒体を提供することにある。

**【0004】**

【課題を解決するための手段】第 1 の観点では、本発明は、利用者が電子化情報を公正な立場と認められる第三者機関に寄託し、第三者機関が前記電子化情報を保管すると共に内容が変更されていないことを保証して当該保管されている電子化情報を利用者に提供することを特徴とする電子化情報保証方法を提供する。上記第 1 の観点による電子化情報保証方法では、公正な立場と認められる第三者機関が電子化情報を保管するため、内容が変更されていないことを保証して当該保管されている電子化情報を利用者に提供することが出来る。よって、例えば契約書を電子化して寄託しておけば、当事者が保有している契約書の内容が契約後に改竄されていないことを何時でも確認できるようになり、取引の安全性を確保できるようになる。

【0005】第 2 の観点では、本発明は、利用者が電子化情報を公正な立場と認められる第三者機関に寄託し、第三者機関が前記電子化情報のダイジェストを保管すると共に利用者から保証依頼された電子化情報のダイジェストを生成し前記保管していたダイジェストと照合し一致したときに内容が変更されていないことを利用者に保証することを特徴とする電子化情報保証方法を提供する。上記構成において、ダイジェストとは、電子化情報よりも情報量が少ないが電子化情報の特徴的なパターンを表した値であり、メッセージ・ダイジェストとも呼ばれる。例えば、電子化情報から一方向ハッシュ関数により作成されるハッシュ値である。上記第 2 の観点による

電子化情報保証方法では、公正な立場と認められる第三者機関が電子化情報のダイジェストを保管するため、利用者から保証依頼された電子化情報の内容が寄託されていた電子化情報と一致するか否かを検証できる。すなわち、内容の変更がないことを保証することが出来る。よって、例えば契約書を電子化して寄託しておけば、当事者が保有している契約書の内容が契約後に改竄されていないことを何時でも確認できるようになり、取引の安全性を確保できるようになる。さらに、第三者機関は電子化情報をそのまま保管せずに、そのダイジェストを保管するため、保管の負担を軽減することが出来る。

【0006】第3の観点では、本発明は、利用者から寄託された電子化情報を保管する保管手段と、保管していた電子化情報とその内容が変更されていないことの電子化保証とを含む電子化保証書を発行する電子化保証書発行手段とを具備することを特徴とする保証サーバを提供する。上記第3の観点による保証サーバを用いれば、上記第1の観点による電子化情報保証方法を好適に実施できる。よって、例えば契約書を電子化して寄託しておけば、当事者が保有している契約書の内容が契約後に改竄されていないことを何時でも確認できるようになり、取引の安全性を確保できるようになる。

【0007】第4の観点では、本発明は、利用者から寄託された電子化情報のダイジェストを生成し保管する保管手段と、利用者から保証依頼された電子化情報のダイジェストを生成し前記保管していたダイジェストと照合し一致したときに内容が変更されていないことを保証する電子化保証書を発行する電子化保証書発行手段とを具備することを特徴とする保証サーバを提供する。上記第4の観点による保証サーバを用いれば、上記第2の観点による電子化情報保証方法を好適に実施できる。よって、例えば契約書を電子化して寄託しておけば、当事者が保有している契約書の内容が契約後に改竄されていないことを何時でも確認できるようになり、取引の安全性を確保できるようになる。

【0008】第5の観点では、本発明は、上記第3または第4の観点により保証サーバにおいて、前記保管手段は、電子化情報またはダイジェストを暗号化して保管すると共に異なる暗号方式により暗号化し直して保管し直すことが可能であることを特徴とする保証サーバを提供する。上記第5の観点による保証サーバでは、電子化情報またはダイジェストを暗号化して保管するため、保管中に内容が改竄されてしまうことを防止できる（どこを改竄すればよいか判らなくなる）。また、現在使用している暗号方式の解読方法が発見されてしまう可能性があるが、解読方法が発見されていない暗号方式により暗号化し直して保管し直すことが可能であるため、安全性を確保することが出来る。

【0009】第6の観点では、本発明は、利用者から寄託された電子化情報を保管する保管手段と、保管してい

た電子化情報とその内容が変更されていないことの電子化保証とを含む電子化保証書を発行する電子化保証書発行手段とをコンピュータに実現させる保証サーバプログラムを記録した、コンピュータ読み取り可能な記録媒体を提供する。上記第6の観点による記録媒体に記録された保証サーバプログラムをコンピュータに読み取らせれば、上記第3の観点による保証サーバを実現できる。

【0010】第7の観点では、本発明は、利用者から寄託された電子化情報のダイジェストを生成し保管する保管手段と、利用者から保証依頼された電子化情報のダイジェストを生成し前記保管していたダイジェストと照合し一致したときに内容が変更されていないことを保証する電子化保証書を発行する電子化保証書発行手段とをコンピュータに実現させる保証サーバプログラムを記録した、コンピュータ読み取り可能な記録媒体を提供する。上記第7の観点による記録媒体に記録された保証サーバプログラムをコンピュータに読み取らせれば、上記第4の観点による保証サーバを実現できる。

【0011】

【発明の実施の形態】以下、図に示す本発明の実施形態により本発明をさらに説明する。なお、これにより本発明が限定されるものではない。

【0012】—第1の実施形態—

図1は、保証サーバH100が、社会的に信用のある証明サーバC100から、保証サーバ証明書HCと証明サーバ公開鍵CKとを受け取る作業の説明図である。保証サーバH100は、証明サーバC100に対して、必要な書類（法人登記簿など）と保証サーバ情報（保証サーバ名称など）HIと保証サーバ公開鍵HKとを渡して、保証サーバ証明書HCの発行を申請する。証明サーバC100は、保証サーバ情報HIと保証サーバ公開鍵HKとを合成して合成情報Ghcを作成する（C1）。次に、その合成情報Ghcからハッシュ関数を用いてハッシュ値を算出し、証明サーバ秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して証明サーバ署名CShを作成する（C2）。次に、合成情報Ghcと証明サーバ署名CShを合成し（C3）、保証サーバ証明書HCを作成し、保証サーバH100に渡す。同時に、証明サーバ公開鍵CKも保証サーバH100に渡す。

【0013】図2は、利用者装置U100が証明サーバC100から利用者証明書UCと証明サーバ公開鍵CKとを受け取る作業の説明図である。利用者装置U100は、証明サーバC100に対して、必要な書類と利用者情報（利用者名称など）UIと利用者公開鍵UKとを渡して、利用者証明書UCの発行を申請する。証明サーバC100は、利用者情報UIと利用者公開鍵UKとを合成して合成情報Gucを作成する（C11）。次に、その合成情報Gucからハッシュ関数を用いてハッシュ値を算出し、証明サーバ秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して証明サーバ署名CSuを作成す

る (C12)。次に、合成情報Gucと証明サーバ署名CSuを合成し (C13)、利用者証明書UCを作成し、利用者装置U100に渡す。同時に、証明サーバ公開鍵CKも利用者装置U100に渡す。

【0014】図3は、利用者装置U100が保証サーバH100に接続する作業の説明図である。利用者装置U100と保証サーバH100とにより電子化情報保証システム100が構成されている。保証サーバH100の機能は、保証サーバプログラムを記録した記録媒体をコンピュータが読み込んで実現する。同様に、利用者装置U100もコンピュータであり、利用者装置U100と保証サーバH100とは通信回線で接続されている。利用者装置U100は、保証サーバH100に対して接続要求Rcを送り、保証サーバH100から応答として返されてくる保証サーバ証明書HCを受け取る。次に、保証サーバ証明書HCを合成情報Ghcと証明サーバ署名CShに分解し (U1)、合成情報Ghcからハッシュ関数によりハッシュ値を求め (U2)、証明サーバ署名CShを証明サーバ公開鍵CKを用いた公開鍵暗号により復号化してハッシュ値に戻し (U3)、2つのハッシュ値を照合して証明サーバC100の署名を確認する (U4)。証明サーバC100の署名が確認できたら、合成情報Ghcを保証サーバ情報HIと保証サーバ公開鍵HKとに分解する (U5)。証明サーバC100の署名が確認できなければ、処理を打ち切る (以下、同様)。次に、保証サーバ情報HIを確認し (U6)、誤りがなければ利用者証明書UCを保証サーバH100に送る。誤りがあれば処理を打ち切る (以下、同様)。

【0015】図4は、保証サーバH100が利用者装置U100の接続を受け入れる作業の説明図である。保証サーバH100は、利用者装置U100から接続要求Rcを受け取ると、応答として保証サーバ証明書HCを返す。次に、利用者装置U100から送られてくる利用者証明書UCを受け取る。次に、利用者証明書UCを合成情報Gucと証明サーバ署名CSuに分解し (H1)、合成情報Gucからハッシュ関数によりハッシュ値を求め (H2)、証明サーバ署名CSuを証明サーバ公開鍵CKを用いた公開鍵暗号により復号化してハッシュ値に戻し (H3)、2つのハッシュ値を照合して証明サーバC100の署名を確認する (H4)。証明サーバC100の署名が確認できたら、合成情報Gucを利用者情報UIと利用者公開鍵UKとに分解する (H5)。次に、利用者情報UIを確認し (H6)、誤りがなければ利用者装置U100の接続を受け入れる。

【0016】図5は、利用者装置U100が保証サーバH100に電子化情報 (以下、寄託データという) を寄託する作業の説明図である。利用者装置U100は、寄託データDDからハッシュ関数を用いてハッシュ値を算出し、利用者秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して利用者署名USdを作成する (U1

2)。次に、寄託データDDと利用者署名USdを合成し (U13)、寄託署名データSDUを作成し、保証サーバH100に送る。次に、保証サーバH100から応答として返されてくる受託署名データSDHを受け取る。次に、受託署名データSDHを合成データGhdと受託署名HSdに分解し (U21)、合成データGhdからハッシュ関数によりハッシュ値を求め (U22)、受託署名HSdを保証サーバ公開鍵HKを用いた公開鍵暗号により復号化してハッシュ値に戻し (U23)、2つのハッシュ値を照合して保証サーバH100の署名を確認する (U24)。保証サーバH100の署名が確認できたら、合成データGhdを保証情報 (受託時のタイムスタンプなど) CIと寄託署名データSDUとに分解する (U25)。保証サーバH100の署名が確認できなければ、処理を打ち切る (以下、同様)。次に、保証情報CIを確認する (U26)。また、分解して得た寄託署名データSDUが送ったものと一致するか照合する (U27)。さらに、受託署名HSdを保存しておく (U28)。

【0017】図6は、保証サーバH100が利用者装置U100からの寄託データDDを保管する作業の説明図である。保証サーバH100は、利用者装置U100から送られてくる寄託署名データSDUを受け取る。次に、寄託署名データSDUを寄託データDDと利用者署名USdに分解し (H11)、寄託データDDからハッシュ関数によりハッシュ値を求め (H12)、利用者署名USdを利用者公開鍵UKを用いた公開鍵暗号により復号化してハッシュ値に戻し (H13)、2つのハッシュ値を照合して利用者の署名を確認する (H14)。利用者の署名が確認できなければ、処理を打ち切る (以下、同様)。利用者の署名が確認できたら、寄託署名データSDUと保証情報CIとを合成し、合成データGhdを作成する (H21)。次に、合成データGhdからハッシュ関数を用いてハッシュ値を算出し、保証サーバ秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して受託署名HSdを作成する (H22)。次に、合成データGhdと受託署名HSdを合成して、受託署名データSDHを作成する (H23)。そして、受託署名データSDHを利用者装置U100に送ると共に、内部的に用いる暗号方式により暗号化し且つ受託署名HSdと対応付けて保管DBに保管する。なお、定期的または不定期的に、その時に解読方法が事実上発見されていない最新の暗号方式により暗号化し直し、保管し直す。

【0018】図7は、利用者装置U100が保証サーバH100に保証書ICの交付を依頼する作業の説明図である。利用者装置U100は、保存していた受託署名HSdからハッシュ関数を用いてハッシュ値を算出し、利用者秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して利用者署名USiを作成する (U32)。次に、受託署名HSdと利用者署名USiを合成し (U3

3)、交付依頼R<sub>i</sub>を作成し、保証サーバH100に送る。次に、保証サーバH100から応答として返されてくる保証書ICを受け取る。次に、保証書ICを合成データG<sub>hi</sub>と保証署名H<sub>Si</sub>に分解し(U41)、合成データG<sub>hi</sub>からハッシュ関数によりハッシュ値を求め

(U42)、保証署名H<sub>Si</sub>を保証サーバ公開鍵HKを用いた公開鍵暗号により復号化してハッシュ値に戻し(U43)、2つのハッシュ値を照合して保証サーバH100の署名を確認する(U44)。保証サーバH100の署名が確認できたら、合成データG<sub>hi</sub>を交付情報(交付時のタイムスタンプなど)I1と受託署名データSDHとに分解する(U45)。次に、受託署名データSDHを合成データG<sub>hd</sub>と受託署名H<sub>Sd</sub>に分解する(U46)。次に、合成データG<sub>hd</sub>を保証情報CIと寄託署名データSDUとに分解する(U47)。次に、寄託署名データSDUを寄託データDDと利用者署名US<sub>d</sub>に分解する(U48)。かくして、利用者は、内容に変更がないことを保証サーバH100が保証した寄託データDDを得ることが出来る。なお、利用者は、自己の利用者署名US<sub>d</sub>があるため、内容に変更がない旨の保証サーバH100の保証を否定することは出来ない。

【0019】図8は、保証サーバH100が利用者装置U100に保証書ICを交付する作業の説明図である。保証サーバH100は、利用者装置U100から送られてくる交付依頼R<sub>i</sub>を受け取る。次に、交付依頼R<sub>i</sub>を受託署名H<sub>Sd</sub>と利用者署名US<sub>i</sub>に分解し(H31)、受託署名H<sub>Sd</sub>からハッシュ関数によりハッシュ値を求め(H32)、利用者署名US<sub>i</sub>を利用者公開鍵UKを用いた公開鍵暗号により復号化してハッシュ値に戻し(H33)、2つのハッシュ値を照合して利用者の署名を確認する(H44)。利用者の署名が確認できたら、受託署名H<sub>Sd</sub>をキーとして保管DBを検索し、対応するデータを取り出し、内部的に用いる暗号方式により復号化して受託署名データSDHを得る(H35)。次に、受託署名データSDHと交付情報I1とを合成し、合成データG<sub>hi</sub>を作成する(H41)。次に、合成データG<sub>hi</sub>からハッシュ関数を用いてハッシュ値を算出し、保証サーバ秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して保証署名H<sub>Si</sub>を作成する(H42)。次に、合成データG<sub>hi</sub>と保証署名H<sub>Si</sub>を合成して、保証書ICを作成する(H43)。そして、保証書ICを利用者装置U100に送る。

【0020】以上の第1の実施形態の電子化情報保証システム100によれば、過去に作成した電子化情報(寄託データDD)の内容が変更されていないことを保証サーバH100が利用者(U100)に保証することが出来る。

【0021】なお、上記第1の実施形態では、利用者装置U100から保証サーバH100への接続作業と寄託作業とを順に行ったが、次の第2の実施形態で説明する

ように同時に行ってもよい。

#### 【0022】-第2の実施形態-

利用者装置U200と保証サーバH200とにより電子化情報保証システム200が構成されている。保証サーバH200の機能は、保証サーバプログラムを記録した記録媒体をコンピュータが読み込んで実現する。同様に、利用者装置U200もコンピュータであり、利用者装置U200と保証サーバH200とは通信回線で接続されている。図9は、利用者装置U200が保証サーバH200に接続すると同時に電子化情報(以下、寄託データという)を寄託する作業の説明図である。U12~U13は、図5のU12~U13と同じであり、寄託データDDからハッシュ関数を用いてハッシュ値を算出し、利用者秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して利用者署名US<sub>d</sub>を作成し(U12)、寄託データDDと利用者署名US<sub>d</sub>を合成し(U13)、寄託署名データSDUを作成する。次に、寄託署名データSDUと利用者証明書UCとを合成し(U51)、証明寄託署名データXDを作成し、保証サーバH200に送る。次に、保証サーバH200から応答として返されてくる証明受託署名データYDを受け取る。次に、証明受託署名データYDを受託署名データSDHと保証サーバ証明書HCに分解する(U61)。U1~U5は、図3のU1~U6と同じであり、保証サーバ証明書HCを合成情報G<sub>hc</sub>と証明サーバ署名CS<sub>h</sub>に分解し(U1)、合成情報G<sub>hc</sub>からハッシュ関数によりハッシュ値を求め(U2)、証明サーバ署名CS<sub>h</sub>を証明サーバ公開鍵CKを用いた公開鍵暗号により復号化してハッシュ値に戻し(U3)、2つのハッシュ値を照合して証明サーバC100の署名を確認し(U4)、合成情報G<sub>hc</sub>を保証サーバ情報H1と保証サーバ公開鍵HKとに分解し(U5)、保証サーバ情報H1の内容を確認する(H6)。U21~U28は、図5のU21~U28と同じであり、受託署名データSDHを合成データG<sub>hd</sub>と受託署名H<sub>Sd</sub>に分解し(U21)、合成データG<sub>hd</sub>からハッシュ関数によりハッシュ値を求め(U22)、受託署名H<sub>Sd</sub>を保証サーバ公開鍵HKを用いた公開鍵暗号により復号化してハッシュ値に戻し(U23)、2つのハッシュ値を照合して保証サーバH200の署名を確認し(U24)、合成データG<sub>hd</sub>を保証情報(受託時のタイムスタンプなど)CIと寄託署名データSDUとに分解し(U25)、保証情報CIを確認し(U26)、分解して得た寄託署名データSDUが送ったものと一致するか照合し(U27)、受託署名H<sub>Sd</sub>を保存しておく(U28)。さらに、合成データG<sub>hd</sub>を保存しておく(U68)。

【0023】図10は、保証サーバH200が利用者装置U200の接続を許可すると共に寄託データDDのハッシュ値を暗号化して保管する作業の説明図である。保証サーバH200は、利用者装置U200から送られて

くる証明寄託署名データXDを寄託署名データSDUと利用者証明書UCに分解する(H51)。H1~H6は、図4のH1~H6と同じであり、利用者証明書UCを合成情報Gucと証明サーバ署名CSuに分解し(H1)、合成情報Gucからハッシュ関数によりハッシュ値を求め(H2)、証明サーバ署名CSuを証明サーバ公開鍵CKを用いた公開鍵暗号により復号化してハッシュ値に戻し(H3)、2つのハッシュ値を照合して証明サーバC100の署名を確認し(H4)、合成情報Gucを利用者情報UIと利用者公開鍵UKとに分解し(H5)、利用者情報UIを確認し(H6)、誤りがなければ利用者装置U200の接続を許可する。H11~H14は、図6のH11~H14と同じであり、寄託署名データSDUを寄託データDDと利用者署名USdに分解し(H11)、寄託データDDからハッシュ関数によりハッシュ値を求め(H12)、利用者署名USdを利用者公開鍵UKを用いた公開鍵暗号により復号化してハッシュ値に戻し(H13)、2つのハッシュ値を照合して利用者の署名を確認する(H14)。H21~H23は、図6のH21~H23と同じであり、寄託署名データSDUと保証情報CIとを合成し、合成データGhdを作成し(H21)、合成データGhdからハッシュ関数を用いてハッシュ値を算出し、保証サーバ秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して受託署名HSdを作成し(H22)、合成データGhdと受託署名HSdを合成して、受託署名データSDHを作成する(H23)。次に、合成データGhdからハッシュ関数を用いてハッシュ値を算出し(H57)、内部的に用いる暗号方式により暗号化し(H58)、受託署名HSdと対応付けて保管DBに保管する。なお、定期的または不定期的に、その時に解読方法が事実上発見されていない最新の暗号方式により暗号化し直し、保管し直す。さらに、受託署名データSDHと保証サーバ証明書HCとを合成し(H59)、証明受託署名データYDを作成して利用者装置U200に送る。

【0024】図11は、利用者装置U200が保証サーバH200に寄託データDDの内容が変更されていないことの保証を依頼する作業の説明図である。利用者装置U200は、保存していた受託署名HSdと合成データGhdとを合成し(U71)、保証依頼データGvdを作成する。次に、保証依頼データGvdからハッシュ関数を用いてハッシュ値を算出し、利用者秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して利用者署名USvを作成する(U72)。次に、保証依頼データGvdと利用者署名USvを合成し(U73)、保証依頼VDを作成し、保証サーバH200に送る。次に、保証サーバH200から応答として返されてくる保証結果VRを受け取る。次に、保証結果VRを合成情報Ghvと保証署名HSvに分解し(U81)、合成情報Ghvからハッシュ関数によりハッシュ値を求め(U82)、保証

署名HSvを保証サーバ公開鍵HKを用いた公開鍵暗号により復号化してハッシュ値に戻し(U83)、2つのハッシュ値を照合して保証サーバH200の署名を確認する(U84)。保証サーバH200の署名が確認できたら、合成情報Ghvを交付情報IIと照合結果Rとに分解する(U85)。かくして、利用者は、内容に変更がないことを保証サーバH200が保証した照合結果Rを得ることが出来る。

【0025】図12は、保証サーバH200が利用者装置U200に保証結果VRを交付する作業の説明図である。保証サーバH200は、利用者装置U200から送られてくる保証依頼VDを受け取る。次に、保証依頼VDを保証依頼データGvdと利用者署名USvに分解し(H81)、保証依頼データGvdからハッシュ関数によりハッシュ値を求め(H82)、利用者署名USvを利用者公開鍵UKを用いた公開鍵暗号により復号化してハッシュ値に戻し(H83)、2つのハッシュ値を照合して利用者の署名を確認する(H84)。利用者の署名が確認できたら、保証依頼データGvdを合成データGhdと受託署名HSdに分解する(H85)。次に、合成データGhdからハッシュ関数によりハッシュ値を求める(H86)。また、受託署名HSdをキーとして保管DBを検索し、対応するデータを取り出し、内部的に用いる暗号方式により復号化してハッシュ値を得る(H87)。次に、合成データGhdから求めたハッシュ値と復号したハッシュ値を照合し(H88)、照合結果Rを作成する。次に、照合結果Rと交付情報IIとを合成し、合成情報Ghvを作成する(H91)。次に、合成情報Ghvからハッシュ関数を用いてハッシュ値を算出し、保証サーバ秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して保証署名HSvを作成する(H92)。次に、合成情報Ghvと保証署名HSvを合成して、保証結果VRを作成する(H93)。そして、保証結果VRを利用者装置U200に送る。

【0026】以上の第2の実施形態の電子化情報保証システム200によれば、過去に作成した寄託データDDの内容が変更されていないことを保証サーバH200が利用者装置U200に保証することが出来る。さらに、保証サーバH200は、寄託データDDをそのまま保管せずに、そのハッシュ値を保管するため、保管の負担を軽減することが出来る。

【0027】なお、上記第2の実施形態では、利用者装置U200から保証サーバH200への接続作業と寄託作業とを同時に行ったが、先述した第1の実施形態で説明したように順に行ってもよい。

【0028】

【発明の効果】本発明の電子化情報保証方法によれば、過去に作成した電子化情報の内容が変更されていないことを公正な第三者機関が保証するため、取引の安全性を確保できるようになる。また、本発明の保証サーバによ

れば、寄託された電子化情報の内容が変更されていないことを利用者に保証することが出来る。更に、本発明の保証サーバプログラムを記録した記録媒体によれば、上記保証サーバの機能をコンピュータに実現させることが出来る。

【図面の簡単な説明】

【図 1】保証サーバが証明サーバから保証サーバ証明書と証明サーバ公開鍵とを受け取る作業の説明図である。

【図 2】利用者装置が証明サーバから利用者証明書と証明サーバ公開鍵とを受け取る作業の説明図である。

【図 3】利用者装置が保証サーバに接続する作業の説明図である。

【図 4】保証サーバが利用者装置の接続を受け入れる作業の説明図である。

【図 5】利用者装置が保証サーバに電子化情報を寄託する作業の説明図である。

【図 6】保証サーバが利用者装置からの寄託データを保管する作業の説明図である。

【図 7】利用者装置が保証サーバに保証書の交付を依頼する作業の説明図である。

【図 8】保証サーバが利用者装置に保証書を交付する作業の説明図である。

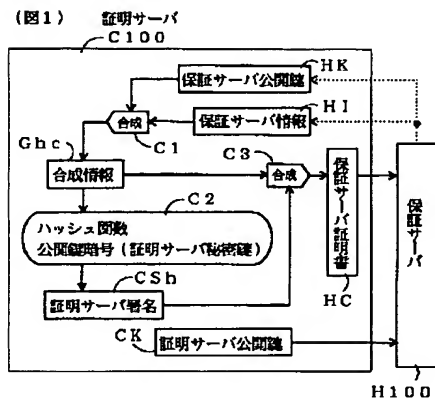
【図 9】利用者装置が保証サーバに接続すると同時に電子化情報を寄託する作業の説明図である。

【図 10】保証サーバが利用者装置の接続を許可すると共に寄託データのハッシュ値を暗号化して保管する作業の説明図である。

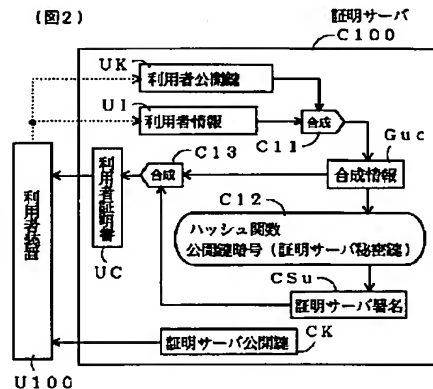
【図 11】利用者装置が保証サーバに寄託データの内容が変更されていないことの保証を依頼する作業の説明図である。

【図 12】保証サーバが利用者装置に保証結果を交付する作業の説明図である。

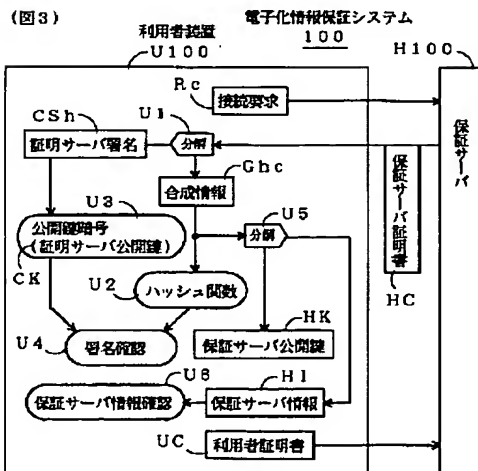
【図 1】



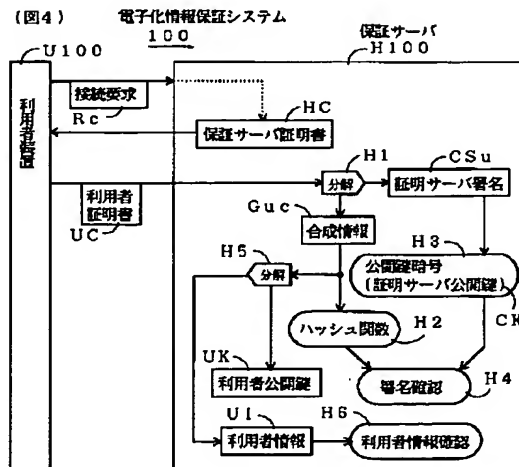
【図 2】



【図 3】

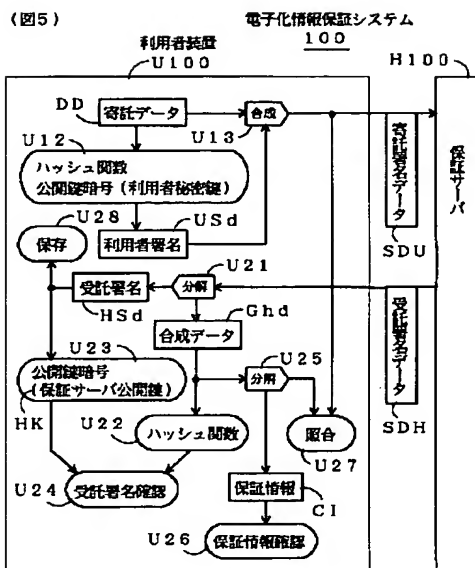


【図 4】

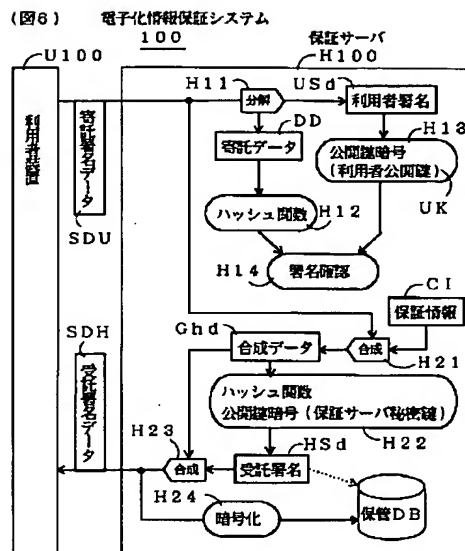




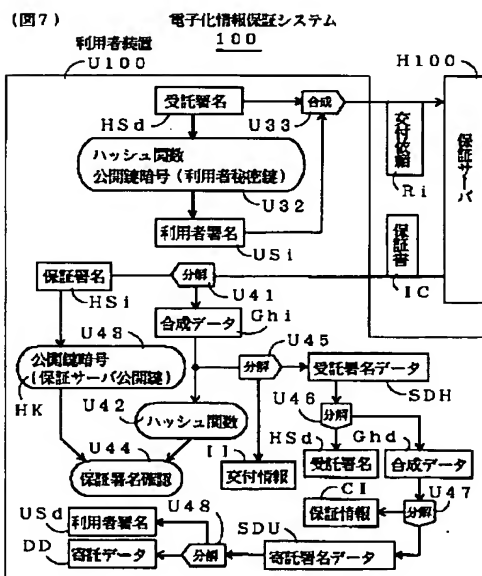
【圖 5】



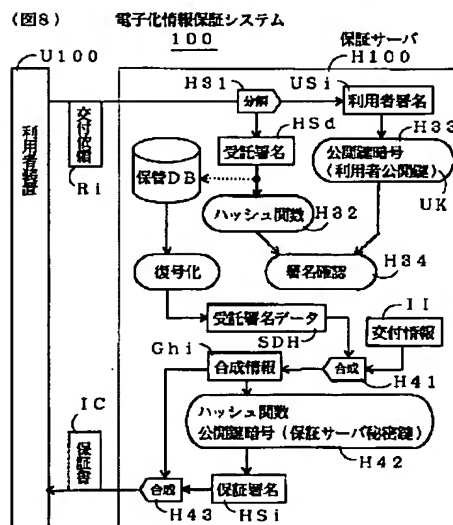
【図 6】



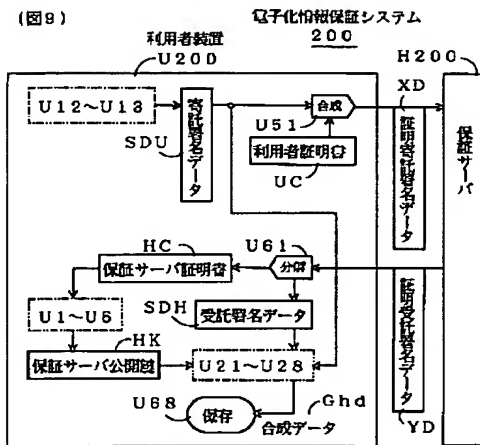
【图 7】



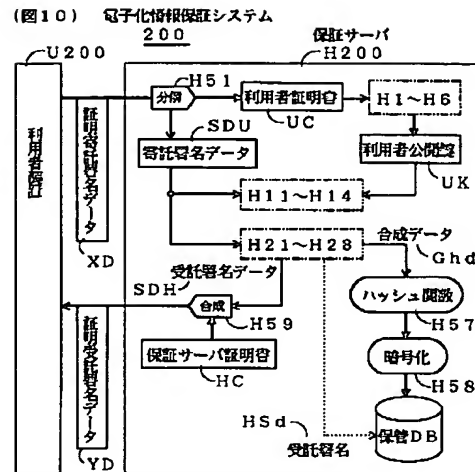
【图 8】



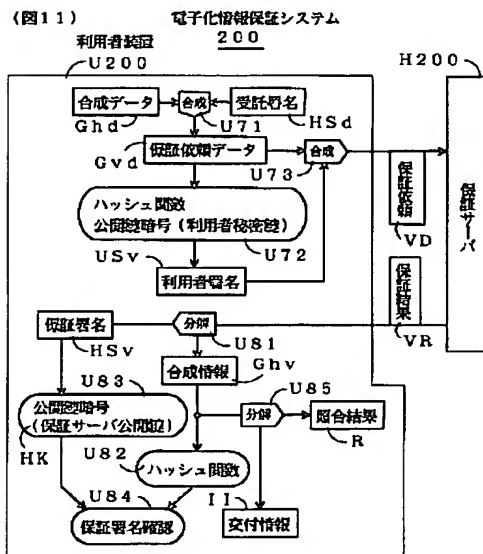
【図 9】



【図 10】



【図 11】



【図 12】

